SOMMAIRE

INTRODUCTION

Il est commun de désigner l'internet des objets comme étant le web 3.0, synonyme d'une troisième révolution. En effet, si la première forme du web éclose dans les années 90 était celle des pages de contenus liés, la seconde plus récente était incarnée par la démocratisation des réseaux sociaux. Le point commun de ces deux premières formes de web est qu'elles ont radicalement bouleversé le droit dans toute sa diversité. Il est donc aisé d'envisager un nouveau bouleversement face à l'avènement prochain de l'internet des objets et notamment en matière de droit des données personnelles.

Selon la Commission Européenne, l'internet des objets se compose d'une « *série de nouveaux systèmes indépendants fonctionnant avec leurs propres infrastructures qui reposent en partie sur les infrastructures existantes de l'internet* ».[1] Ces systèmes indépendants, ce sont ces objets connectés dont le succès ne cesse de croitre ces derniers temps. En effet, si l'internet des objets connaît déjà ses prémices, les prévisions annoncées laissent entrevoir une croissance exponentielle et de réels bouleversements. Selon ces prévisions[2], d'ici 2018 chaque personne possèdera en moyenne 8 objets connectés. Rien d'étonnant lorsqu'on voit les évolutions actuelles qui font de chaque objet du quotidien un potentiel objet connecté. Ceci est le cas notamment des montres, des lunettes, des tee-shirts, des voitures ou autres chaussures connectées. La fonction principale de ces différents objets connectés et de capter les données personnelles de leurs utilisateurs afin de leur apporter un service adapté à leur profil.

Par données personnelles, on entend au sens de l'article 2 de la loi 78-12 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés : « *tout information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement* ». Ainsi, si nous prenons l'exemple du bracelet connecté, l'objet le plus iconique en la matière, ce dernier est doté d'un capteur capable de collecter toutes sortes de données personnelles. En effet, ce dernier peut capter le rythme cardiaque d'une personne pour lui conseiller d'aller consulter un médecin ou encore capter sa géolocalisation pour lui communiquer des informations météorologiques. Le rythme cardiaque et la géolocalisation sont des exemples de deux types d'informations permettant d'identifier directement ou indirectement une personne et constituant ainsi des données personnelles.

Ces données personnelles collectées par les objets connectés représentent une manne financière considérable. Selon certaines estimations, le marché français des objets connectés pesait déjà 150 millions d'euros en 2013 et devrait représenter 500 millions d'euros en 2016[3]. Les données personnelles sont le véritable nerf de la guerre, le « pétrole numérique » de ce web 3.0, car comme l'or noir, un traitement est nécessaire pour en retirer toute sa richesse.

---

[1] Commission Européenne, *L'internet des objets : un plan d'action pour l'Europe,* COM/2009/0278, 18 juin 2009*,* p. 2

[2] DE SILGUY (S.), *Les objets connectés, un risque pour la protection de nos données personnelles*, RDLC, octobre 2014, numéro

[2] DE SILGUY (S.), *Les objets connectés, un risque pour la protection de nos données personnelles*, RDLC, octobre 2014, numéro 119, p. 69

[3] FREDOUELLE (A.), « Le marché français des objets connectés pèsera 500 millions en 2016 », *journaldunet.com, 2 mai 2014.*

En effet, le volume des données collectées est si important qu'il est indispensable d'opérer un tri dans cet amas considérable de données appelé le Big Data. À ce titre, en 2013, chaque foyer produit en moyenne assez de données pour remplir 65 Iphones de 32 gigaoctets, et selon les dernières prévisions, il en faudra 318 en 2020[4]. L'internet des objets participera donc plus que jamais à un partage massif de données personnelles du fait de ces interactions accrues avec des objets connectés toujours plus nombreux. Ces données, les objets connectés vont les utiliser mais aussi les communiquer, ce qui est la base de l'internet des objets. Le risque est donc un éparpillement massif dans le monde entier des données personnelles captées par ces périphériques. Au regard, du caractère intrusif de telles technologies et de la valeur économique de ces données personnelles, des pratiques abusives sont donc à prévoir dans le cadre de l'internet des objets aux dépens des utilisateurs.

En effet, des abus en matière de données personnelles existent depuis déjà longtemps, comme l'illustre l'exemple historique du fichier SAFARI. En 1970, le gouvernement français a eu pour projet d'identifier chaque citoyen par un numéro. Suite à l'émoi qu'a pu provoquer l'annonce d'une telle mesure à l'époque, il est apparu nécessaire de légiférer autour de la protection des données personnelles, afin de réguler la gestion des informations personnelles. Ainsi, le 6 janvier 1978 est entré en vigueur la loi relative à l'informatique, aux fichiers et aux libertés, instituant la Commission Nationale de l'Informatique et des Libertés. Depuis, cette loi a été modifiée par la loi du 6 août 2004 qui a transposé en France la directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes à l'égard des données personnelles. À l'heure actuelle, ces textes constituent le socle du droit de la protection des données personnelles.

Cependant, l'internet des objets tend à remettre en question cette protection des données personnelles. En effet, récemment, le groupe de travail de l'article 29 qui regroupe toutes les CNIL européenne, a adopté un avis relatif aux « *Récents développements de l'internet des objets* »[5]. Dans cet avis, le G29 a identifié différents types de problèmes relatifs à la protection des données personnelles pouvant résulter de l'internet des objets. Parmi les difficultés identifiées par le groupe de travail on peut notamment citer : un profilage intrusif, le caractère aléatoire de l'anonymat ou encore l'absence de contrôle de l'utilisateur sur la diffusion de ses données.

Ainsi, les problèmes pointés du doigt par le groupe du G29 nous pousse à nous interroger sur le caractère efficient du cadre législatif relatif aux données personnelles face à l'internet des objets. En d'autres termes, le droit des données personnelles permet-il un encadrement suffisant face à l'avènement de l'internet des objets ?

Pour tenter de répondre à cette question, nous allons dans un premier temps identifier plus en profondeur les menaces potentielles relatives aux données personnelles générées par l'internet des objets (section 1). Puis, dans un deuxième temps nous étudierons le cadre législatif relatif à la protection des données personnelles en pointant du doigt ses insuffisances

[4] DE SILGUY (S.), *op.cit,* p. 69
[5] G29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, avis du 16 septembre 2014, 24 p.

face à l'internet des objets (section 2). Enfin, dans un troisième temps nous étudierons le projet de règlement européen relatif à la protection des données personnelles qui devrait répondre aux carences de cette protection des données personnelles par le droit et vivement impacter les acteurs de l'internet des objets (Section 3).

SECTION I/ L'INTERNET DES OBJETS, UNE MENACE POTENTIELLE POUR LES DONNÉES PERSONNELLES

Face à la révolution du web 3.0 et de l'utilisation massive des nouveaux objets dits «intelligents », la question de la protection des données personnelles est on ne peut plus actuelle de nos jours. On en veut pour preuve les nombreuses rencontres qui se sont emparées du sujet. Citons pour exemple, au niveau régional, le colloque MÉDIAS014 « Is 'Big Data' beautiful ? », organisé le 12 décembre dernier par notre université AMU (Aix-Marseille Université). Mais encore, au niveau national, la conférence organisée par la CNIL et le G29 (Groupe européen des autorités de protection des données) le 8 décembre 2014, sous le nom de l'« *European data governance forum* ». En effet, le thème principal abordé lors de cette rencontre était la protection des données des citoyens européens.

Nous étudierons dans cette première section la menace potentielle que peut représenter l'internet des objets pour les données personnelles, tout d'abord par son caractère intrusif (I), puis par son caractère vulnérable (II).

I/ Le caractère intrusif de l'internet des objets, vecteur de risques potentiels pour les données personnelles

Dans ce premier paragraphe, notre étude se concentrera notamment sur le caractère d'ubiquité des données personnelles (A), puis sur la question de la finalité d'utilisation des données personnelles (B).

A/ L'ubiquité des données personnelles, conséquence de l'omniprésence des objets connectés

Nul doute que cette protection doit d'ores et déjà être pensée à la lumière du déferlement d'objets connectés sur notre quotidien. Comme différents groupes avant le nôtre l'ont déjà exprimé, les objets connectés deviennent littéralement omniprésents, quelque soit le lieu où nous nous trouvons : maison, travail, en voyage, au restaurant, dans la voiture … En conséquence, les données personnelles collectées sont elles aussi démultipliées, et en tout lieu.

Tout ceci nous amène à évoquer la notion d'ubiquité des données personnelles. L'ubiquité, ou omniprésence, est la « possibilité d'être présent en plusieurs lieux à la fois »[6]. En effet, lorsque nous utilisons un objet connecté, et que ce dernier collecte des données, ces informations peuvent être accessibles en même temps et en plusieurs lieux à la fois : dans la mémoire de l'objet connecté, sur notre smartphone afin que nous puissions les consulter, et

[6] LE PETIT ROBERT, *Le Robert*, Paris, 2013, p. 2651

même parfois chez notre médecin, notre assureur, ou encore la société créatrice de l'objet, où elles sont alors analysées.

Il est donc important d'identifier les difficultés que peuvent créer la diffusion de ces données personnelles vers d'autres récepteurs, ainsi que le caractère instantané du transfert. Que se passerait-il si les données produites par notre objet connecté étaient erronées ? Imaginons que notre médecin ou notre assureur soit informé en temps réel de nos données personnelles, et notamment de celles qui concernent notre santé. Si ces informations sont faussées, à cause d'une défaillance de l'appareil ou encore parce que nous l'avons prêté à une autre personne sans en mesurer les conséquences, alors il y a un risque que le médecin ou l'assureur dans notre exemple prenne des mesures en fonction de données qui ne sont pas la réalité. Le consommateur risque de voir son traitement médical changer alors qu'il n'est pas adapté, ou encore de voir s'envoler le prix de son assurance, car considéré comme un client à risque à tort. C'est ce que l'on peut appeler l'effet pervers de l'ubiquité. Il serait donc nécessaire dans un premier temps que le droit protège le consommateur des défaillances de son objet connecté, et des incidences que cela pourrait avoir. Par ailleurs, la notion d'ubiquité des données personnelles inclue une autre réalité dérangeante : « *supprimer une donnée sur le service où elle a été écrite à l'origine n'implique nullement son effacement sur les multiples autres services où elle a pu être reproduite* »[7]. Il incombera à l'utilisateur d'un objet connecté d'effectuer des démarches en vu de la suppression de ses données, mais rien n'est automatique. Nous reviendrons sur ce point un peu plus tard dans notre exposé.

Il est par ailleurs envisageable de rattacher le caractère d'ubiquité des données personnelles à la question de la finalité de leur utilisation.

B/ La question de la finalité d'utilisation des données personnelles collectées

On touche ici à une notion importante qui est celle de la finalité d'utilisation des données personnelles collectées. En tant que consommateur, que savons nous réellement de l'utilisation qui est faite de nos données ? Lorsque nous acceptons les conditions générales d'utilisation d'un objet connecté, est-on certain que les données collectées par l'appareil ne seront pas revendues, exploitées à des fins commerciales ? Est-on certain que ces informations ne sont délivrées qu'au fabricant de l'objet connecté, et qu'elles ne servent qu'au bon usage de l'objet acquis ? Malheureusement, il existe un manque d'information patent quant à la finalité d'utilisation de la collecte de ces données. C'est un fait qu'ont souligné les instances de protection des données européennes comme le Groupe de l'article 29 (ou G29) lors de l'« *European data governance forum* ». Pire encore, nous sommes tributaires de cette collecte de données, sans laquelle la plupart des objets connectés refusent de fonctionner … C'est un cercle vicieux dans lequel le consommateur se retrouve contraint d'accepter bien malgré lui, et sans grandes précisions, que ses données personnelles soient collectées, puis

[7] LEROY (F.), *Réseaux sociaux & Cie – Le commerce des données personnelles*, Actes sud, Arles, 2013, p. 245

décortiquées par un organisme ou une entreprise. En effet, les données ont une valeur inestimable pour les entreprises, car elles leur permettent de mieux connaître leurs clients et leur mode de vie[8]. Pour Michel Gentot (Conseiller d'État), l'offre de masse s'est aujourd'hui individualisée grâce à la technique du *one to one*, ou CRM (*customer relationship management*), permettant de cibler précisément l'offre commerciale à utiliser[9] grâce à l'analyse de données numériques. Ces informations aideront par exemple les entreprises à pratiquer le *retargeting*, ou reciblage publicitaire[10]. Cela peut se traduire par l'affichage d'une bannière publicitaire après analyse des recherches de navigation d'un internaute à la recherche d'un produit en particulier.

Confronté à cette réalité, le G29 a adopté un avis sur les récents développements de l'internet des objets le 16 septembre 2014, afin de rappeler dans un premier temps que ces derniers sont soumis à la législation européenne, et notamment à la directive européenne 95/46/CE, en ce qu'ils collectent et traitent des données personnelles. Les CNIL européennes ont remarqué à l'occasion de cet avis que l'internet des objets pose à la fois des questions traditionnelles et d'autres plus nouvelles en matière de protection des données personnelles. C'est pour cela qu'en raison de la vitesse de leur propagation, il semble urgent qu'un ensemble de recommandations soient définies et transmises aux différents acteurs concernés (Le responsable du traitement et le consommateur d'objets connectés). L'avis du G29 déplore à ce sujet un certain nombre de difficultés dans un paragraphe nommé « *Privacy and data protection challenges related to the Internet of Things* ». Parmi ces challenges, le G29 dénonce un manque de contrôle, une asymétrie de l'information, ainsi qu'une faible qualité du consentement de l'utilisateur d'un objet connecté.

Tout d'abord, en ce qui concerne le manque de contrôle et l'asymétrie de l'information[11] : les consommateurs ne sont pas assez renseignés sur les informations qu'ils partagent, et peuvent perdre facilement le contrôle de leurs données. Selon une enquête réalisée par Havas Media, 83,6% des internautes sont inquiets des usages qui peuvent être faits de leurs données. S'ils estiment être prêts à communiquer sur leurs centres d'intérêts ou des données anonymisées, une majorité d'entre eux ne souhaite pas partager des informations sur leurs coordonnées personnelles, et plus de 90% des internautes estiment la création d'un cadre juridique ou réglementaire nécessaire[12]. Ensuite, l'avis du G29 pointe également du doigt la qualité du consentement de l'utilisateur. En effet, celle-ci peut se révéler extrêmement faible : « *most observers may not distinguish a normal watch from a connected one, when the latter may yet embed cameras, microphones and motion sensors that can record and transfer data without the individuals being aware of, and even less consenting to such processing.* »[13] ; À tel point que les instances de protection des données

[8] REY (B.), *La vie privée à l'ère du numérique*, Lavoisier, Cachan, 2012, p. 153
[9] GENTOT (M.), « la protection des données personnelles à la croisée des chemins », sous la direction de TABATONI (P.), *La protection de la vie privée dans la société d'information*, Tome 3, coll. Cahiers des sciences morales et politiques, PUF, Paris, 2002, p.26
[10] HAAS (G.), et COHEN-HADRIA (Y.), *Guide juridique informatique et libertés – Collecte, traitement et sécurité des données dans l'univers numérique : ce que vous devez savoir*, ENI, Saint-Herblain, 2012, p. 134
[11] G29, *op. cit.,* p. 6
[12] HAVAS MEDIA, *Les français et leurs données personnelles, quelle place pour les marques ?*, septembre 2014, p. 25
[13] G29, *op. cit.*, p. 7

personnelles se demandent si la qualité du consentement, tel qui peut être donné de nos jours, est suffisamment libre pour être valide du point de vue du droit européen. Le problème viendrait du fait que les objets connectés ne fournissent pas en eux-mêmes les informations suffisantes au consommateur pour le rassurer quant à la finalité d'utilisation de ses données personnelles, et ne mettent pas en place un mécanisme interne suffisant pour recueillir un consentement de qualité de la part de l'utilisateur.

Tous ces éléments nous mènent à étudier la vulnérabilité de l'internet des objets face aux risques potentiels pour les données personnelles collectées (2§).

II/ Le caractère vulnérable de l'internet des objets, vecteur de risques potentiels pour les données personnelles

L'aspect sécurité des données personnelles représente une véritable lutte contre le piratage et l'usurpation d'identité (A), dans un monde où le data mining, ou la désanonymisation, fait rage (B).

A/ Les risques de piratage et d'usurpation d'identité

Le piratage des objets connectés grâce aux données personnelles est une autre menace à ne pas négliger. Dorénavant, et comme nous l'avons déjà indiqué précédemment, tout notre quotidien est susceptible d'être connecté. Cette réalité implique que des personnes mal intentionnées puissent s'immiscer dans notre vie privée, via la connexion internet, et qu'elles puissent contrôler nos objets à notre insu. Imaginons un voleur qui souhaite entrer dans une maison. Si ce dernier arrive à prendre connaissance d'un certain nombre d'informations, comme par exemple notre adresse IP, et que l'objet n'est pas protégé par mot de passe (comme la majorité d'entre eux), il pourra contrôler l'objet connecté permettant l'ouverture et le verrouillage de notre domicile avec une grande facilitée …

Un autre exemple avec la voiture connectée. Les constructeurs automobiles souhaitent implanter dans les voitures de demain des mécanismes leurs permettant d'interagir entre elles et de s'échanger des informations (donc des données via internet) afin de fluidifier le trafic, et d'éviter les accidents de la route[14]. Or dès lors qu'un objet est connecté à internet, « *il y a une possibilité de le contrôler à distance* », comme le fit très justement remarquer le directeur du centre de cybercriminalité de l'agence Europol, M. Troels Oerting, lors d'une interview sur la chaîne de télévision américaine CNBC. Le sujet avait d'ailleurs déchainé les passions aux Etats-Unis en juin 2013, alors qu'un journaliste d'investigation, Michael Hastings, avait été retrouvé mort, carbonisé dans sa voiture ultra-connectée. Selon différentes sources, ce dernier faisait l'objet d'une enquête par le FBI est était sur « un gros coup ». Autant de circonstances ayant

[14] DESSIBOURG (O.), « Pirater une voiture ? C'est possible … », *Lemonde.fr*, 4 mars 2014

fait ressurgir une théorie du complot sur l'éventuel hack de la voiture du journaliste[15]. Cette prétendue cyberattaque n'a en l'espèce jamais été prouvée, mais de nombreux spécialistes en cybercriminologie ont affirmé que cette hypothèse était plausible et techniquement réalisable. La voiture connectée ne serait donc plus seulement synonyme de sécurité, mais aussi de possible piratage entre les mains d'une personne mal intentionnée.

Face à ce danger, beaucoup pointent du doigt un moteur de recherche particulier, nommé Shodan. Créé en 2009 par un dénommé John Matherly, il explore, référence et rassemble, non pas des adresses URL accessibles en ligne, mais l'ensemble des objets liés à une connexion internet[16]. Bien que ce moteur de recherche ne soit qu'un simple détecteur d'objets connectés, il représente tout de même le répertoire idéal pour tout pirate informatique. Le risque étant qu'il puisse, à partir de ce site web, repérer un objet et chercher à le contrôler. Cette issue est fortement envisageable lorsque les paramètres de protection de l'objet connecté sont faibles, voir quasi inexistants. Nos données personnelles collectées dans l'objet en question sont alors susceptibles d'être détournées à des fins malveillantes, ce qui soulève une véritable question de sécurité concernant l'utilisation de ces objets dans notre quotidien, mais pas seulement. En effet, le moteur de recherche Shodan référence aussi bien des webcams, des imprimantes, des réfrigérateurs … que des centrales électriques connectées[17] ! En effet, lorsque ces dernières sont sorties de terre, Internet n'en était encore qu'à son balbutiement. Les systèmes de contrôle des centrales ont alors été mis en ligne, sans véritable protection. On imaginait assez mal à l'époque l'ampleur que prendrait le phénomène Internet et les nouveaux risques qu'il engendrerait. C'est ce qu'ont souhaité dévoiler deux journalistes de Rue89, on se connectant à plusieurs webcams et caméras connectées en passant par le moteur de recherche Shodan[18]. En réussissant à obtenir des images en direct chez différentes personnes, pharmacies, et boutiques, les journalistes ont démontré avec quelle facilité il est possible de s'immiscer dans le travail ou l'intimité des individus : « *J'ai ainsi été le témoin de votre vie intime, à votre insu.* ». Un constat glaçant qui illustre parfaitement le risque de surexposition de la vie privée d'un utilisateur d'objet connecté. Selon un récent rapport rendu par la société HP, plus de 70% des objets connectés présentent des vulnérabilités importantes concernant leur système de sécurité[19].

Ces nouvelles menaces pour la sécurité des données personnelles sont également devenues le terrain de jeu des nouveaux usurpateurs d'identité. Selon Jean-Paul Pinte, expert en cybercriminalité, l'usurpation d'identité d'une personne physique ou morale consiste à prendre délibérément l'identité d'une autre personne vivante, dans le but de réaliser des actions frauduleuses[20]. Si le phénomène de l'usurpation d'identité n'est pas nouveau, internet

[15] CHAMPEAU (G.), « Michael Hastings a-t-il été tué par le piratage de sa voiture ? », *numerama.com*, 26 juin 2013
[16] PIROTTE (J.), « Shodan : un moteur de recherche pour l'internet des objets », *objetconnecte.net*, 30 mai 2014
[17] ANONYME, « INTRUSION 2.0 - Avec Shodan, contrôlez des webcams et imprimez chez les autres », *lemonde.fr*, 10 juin 2014
[18] KRISTANADJAJA (G.), « J'ai pris le contrôle de votre caméra et je vous ai retrouvés », *rue89.nouvelobs.com*, 09 juin 2014
[19] HP. FORTIFY SECURITY RESEARCH, *Internet of Things Research Study*, HP report, september 2014, p.4
[20] PINTE (J-P.), « Le vol d'identité, la plus grande menace criminelle des années à venir », *atlantico.fr*, 30 décembre 2013

et le développement des objets connectés ont fortement aggravé la situation. La multiplication des données personnelles se retrouvant sur internet à cause des objets connectés a également multiplié les risques en facilitant l'usurpation d'identité. Aux Etats-Unis, le rapport de la Federal Trade Commission (une agence de surveillance indépendante du gouvernement américain) du 27 janvier 2015 dévoile notamment que le coût attribué aux usurpations d'identité représenterait près de 24,7 trillions de dollars aux États-Unis[21]. L'enjeu est extrêmement important car l'usurpation d'identité est susceptible d'aller bien plus loin que ce dont nous sommes habitué. Grâce, ou à cause des objets connectés, il sera désormais possible d'imiter notre vie privée, notre manière de vivre, notre façon de marcher, ou encore de transférer à un médecin ou toute autre entité des données personnelles sur notre santé, quand bien même elles ne nous appartiendraient pas. Ce qui fait par ailleurs écho à l'effet pervers de l'ubiquité des données personnelles comme nous l'évoquions dans un paragraphe précédent.

Enfin, si l'amplification des risques d'usurpation d'identité et de piratage semble inquiéter les français, près de 49% des consommateurs d'objets connectés restent pourtant prêt à communiquer des informations générales anonymisés comme l'âge, le sexe, ou encore la profession[22]. Le public n'est en effet pas sensibilisé sur la possible désanonymisation susceptible d'être engendrée par le phénomène du data mining.

B/ Les dangers du data mining, ou le phénomène de désanonymisation

Les informations que nous renseignons à notre égard à nos objets connectés (nom de famille, âge, adresse IP, adresse postale …), ne sont pas toujours confidentielles, ou d'une importance capitale si nous les considérons individuellement. Comme d'autres groupes l'ont évoqué avant nous, ces informations peuvent être notre nom, notre adresse postale, notre adresse IP … Mais en réalité, ce ne sont pas forcément les données que nous renseignons, prises individuellement, qui posent problème.

En effet, l'internet des objets est créateur d'un concept que l'on nomme le data mining. Littéralement « l'exploration de données », le data mining peut être défini comme *« la captation et l'exploitation de données triviales, voire insignifiantes par elles-mêmes, mais susceptibles de contribuer à un profilage très fin des individus »*. Et c'est bien ce profilage extrêmement précis, à partir de données toutes simples, qui est susceptible de poser problème en matière d'atteinte à la vie privée. L'identification précise d'une personne, de son comportement, de ses habitudes, de son mode de vie, est alors rendu possible grâce (ou à cause) de cette technologie révolutionnaire. Celle-ci analyse des quantités astronomiques de données, et grâce à des règles statistiques et autres algorithmes mathématiques, le logiciel effectuant cet exploration de données est capable de comparer très minutieusement l'ensemble des résultats obtenus. Il

[21] FTC., *Internet of things - Privacy & security in a connected world,* FTC staff report, january 2015, p.11
[22] HAVAS MEDIA, *op. cit.*, p. 23

peut alors en déduire des corrélations, des ressemblances, des profils types, etc. … Avec le data mining, une multitude de données anonymisées peuvent malgré tout conduire à l'identification parfaite d'une personne[23]. Ainsi, elles peuvent même devenir des données sensibles. La frontière entre les données anonymes et les données personnelles identifiantes est donc remise en cause, et ce qu'une personne pense concéder à une entreprise de manière anonyme fini par dévoiler son identité par un savant croisement de données. On est en droit de se demander si cette pratique ne bafoue pas le consentement des individus, car ce consentement a été donné pour une collecte, et donc un traitement, de données personnelles anonymes. Mais les responsables de ces traitements se cachent actuellement derrière la nature première des données qu'ils ont collectés, c'est à dire derrière le fait que ces données étaient avant tout anonymes. Et ce, même si elles finissent pas ne plus l'être par leur faute. Il paraît donc nécessaire que le législateur ou la jurisprudence viennent trancher sur la qualification à attribuer à des données à l'origine anonymes, puis « désanonymisées » par le data mining.

Autre problème résultant de cette désanonymisation : la catégorisation des individus. Chaque individu est classé dans une catégorie, un profil client type duquel il sera extrêmement difficile de se détacher. Pour Pierre-Jean Benghozi, membre de l'ARCEP et directeur de recherches au CNRS, cette « désanonymisation » combinée à la catégorisation des personnes peut conduire à des discriminations en tout genre. Yves Poullet (directeur du CRID et professeur universitaire Belge) n'hésite plus quant à lui à parler d'une « *problématique de quadrillage à partir de données triviales* »[24].

Tout ce processus d'analyse existe dans un but essentiellement commercial : il permet de faire rentrer un individu dans une case pour établir un profil type, une approche, et une publicité ciblée. Bien souvent pourtant, l'identité de la personne en question est complétement déformée par le logiciel pour correspondre à l'une des cases prédéfinies. L'analyse est donc restrictive, et le résultat tient moins compte de la réalité. On peut alors envisager que dans certains cas, cette compression d'information puisse être dommageable pour la personne concernée. Par exemple, une personne qui figurerait sur une black liste, ou liste noire, perdrait automatiquement son droit à contracter avec les personnes pouvant accéder à la liste. Si cette personne est inscrite sur cette black liste par erreur, cela pourrait donc avoir des conséquences préjudiciables[25].

En conclusion, il paraît donc nécessaire que les consommateurs d'objets connectés et les responsables des traitements de données personnelles soient d'avantage sensibilisés sur le sujet, afin qu'ils puissent conjointement adopter les bons usages pour prévenir et réduire ces menaces potentielles. Les consommateurs d'objets connectés doivent prendre conscience des risques auxquels ils s'exposent s'ils ne prennent pas les mesures nécessaires : « *se sentir ordinaire*

[23] CNIL, *Vie privée à l'horizon 2020*, Cahier IP n°1, p.33
[24] CNIL, *op. cit.,* p. 33
[25] HAAS (G.), et COHEN-HADRIA (Y.), *op. cit.,* p. 151

et noyé dans la masse permettrait ainsi de relativiser la gène occasionnée »[26]. Ce sentiment d'invulnérabilité ne doit pourtant pas se développer. Le premier des conseils à donner aux utilisateurs d'objets connectés doit être de changer le mot de passe, ou d'en créer un lorsqu'il n'existe pas d'office. Mais attention, ce mot de passe doit être assez complexe pour ne pas être facilement identifié. Pour cela, il doit être constitué de chiffres et de lettres, de majuscules ainsi que de minuscules[27]. Oubliez les dates de naissances, les prénoms des enfants, le « password», ou encore le traditionnel « 123456 », qui reste actuellement le mot de passe le plus utilisé dans le monde[28] … La sécurité des données personnelles collectées par l'objet dépend donc en grande partie de la bonne volonté du consommateur éclairé de cette nécessité.

Après avoir mis en exergue les menaces potentielles créées par l'internet des objets envers les données personnelles, nous nous demanderons si le cadre législatif actuellement applicable garantit suffisamment la protection des données personnelles (Section II).

[26] REY (B.), *op. cit.,* p. 130
[27] JUNG (M.), « Apprenez à mieux gérer vos mots de passe », *bfmtv.com*, 27 janvier 2015
[28] BRETON (J.), « Mots de passe les plus utilisés : le top 25 demeure dominé par le 123456 », *lesnumeriques.com*, 21 janvier 2015

SECTION II/ L'INTERNET DES OBJETS, UN ENCADREMENT PERFECTIBLE PAR LE DROIT DES DONNEES PERSONNELLES

Face aux multiples dangers exposés précédemment, inhérents à l'utilisation des objets connectés, il est nécessaire de s'intéresser à la protection des données personnelles dont peuvent se prévaloir les individus.

Le droit offre une protection des données personnelles à travers la loi relative à l'informatique, aux fichiers et aux libertés de 1978. Cette législation a été mise en place afin de renforcer les droits des individus sur leurs données. Cependant, face à l'émergence du numérique, la directive Européenne 95/46/CE a modifié la loi initiale afin d'harmoniser la protection des données personnelles dans les pays membres de l'Union Européenne. C'est seulement le 6 aout 2004 que la France a transposé cette directive. Or, malgré cette avancée en la matière, la protection actuelle semble présenter de nombreuses limites face à la révolution actuelle du web 3.0 et de tous les nouveaux objets dits « intelligents ». A ce titre, le G29 dans un avis du 16 septembre 2014 a fait une série de recommandations dans ce domaine[29] en vue d'une amélioration future de l'encadrement législatif. Parallèlement au G29, la CNIL a fait une série de propositions dans le cadre du projet de numérique, afin de modifier la loi relative à l'informatique, aux fichiers et aux libertés pour la rendre plus effective face aux besoins actuels.

Nous allons voir dans un premier temps en quoi consiste l'encadrement législatif du traitement et de la collecte des données personnelles (I) et dans un second temps, celui relatif aux prétentions des utilisateurs sur leurs données personnelles (II).

I/ L'encadrement législatif du traitement et de la collecte des données personnelles

La loi relative à l'informatique, aux fichiers et aux libertés pose un ensemble de principes impératifs au traitement des données personnelles (A). Le traitement et la collecte sont également encadrés par la mise en place d'un régime contraignant à l'égard du responsable du traitement (B). Cependant, la protection des données reste insuffisante en ce qui concerne la protection des flux transfrontières (C) et en ce qu'elle présente d'importantes carences concernant celle les mineurs (D).

[29] G29, *op. cit.*

A/ Le respect de principes impératifs au traitement des données personnelles

L'article 6 de la loi du 6 janvier 1978 pose ainsi les principes selon lesquels, les données doivent être traitées de manière loyale et licite suivant des finalités déterminées, explicites et légitimes. Celles-ci doivent être collectées et traitées de manière adéquate, pertinente et non excessive ainsi que de façon exacte et complète. Ainsi, toutes les données qui ne répondent pas à ces exigences doivent être effacées. De plus, la conservation de ces données ne doit pas excéder la durée nécessaire aux finalités pour lesquelles elles ont été collectées et traitées. Prenons pour exemple le bracelet connecté de mesures de performances sportives. Ce dernier va collecter les données relatives au rythme cardiaque mais également aux calories brûlées, au temps d'activité et à la distance parcourue mais aussi à la géolocalisation. Cependant, les données relatives à la position géographique de l'utilisateur doivent être effacées en l'application de l'article 6 précité car elles ne correspondent pas à la finalité de cet objet. Le non-respect de ce principe de finalité est sanctionné par l'article 226-21 du Code pénal, qui prévoit une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende. À ce titre, le G29 a, dans son dernier avis, montré une inquiétude quant à la réorientation de la finalité d'origine du traitement des données. En effet, aucune disposition ne prévoit le cas ou la collecte des données suivrait une finalité différente que celle à laquelle l'utilisateur ait consenti. Ainsi, l'utilisateur d'objets connectés, ne se sent pas aujourd'hui suffisamment en confiance.

Parallèlement à l'application de l'article 6, l'article 7 de la loi relative à l'informatique, aux fichiers et aux libertés prévoit un droit au consentement. En effet, tout traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée. Cependant, le G29 dans son dernier rapport du 16 septembre 2014 a montré une faille à ce niveau. Souvent, le consentement éclairé de l'utilisateur n'est pas recueilli de manière explicite, et ce dernier n'a aucun contrôle sur la diffusion de ces données.

La loi encadre également la protection des données personnelles à travers un régime de responsabilité contraignant destiné au responsable du traitement.

B/ Des standards sécuritaires contraignants imposés au responsable du traitement

L'usage des objets connectés révèle des risques importants pouvant aller jusqu'à mettre en danger la vie privée des utilisateurs. Afin d'éviter toute intrusion dans leur intimité, la loi prévoit essentiellement deux obligations à l'égard du responsable du traitement des données.

En effet, l'article 34 prévoit une obligation de sécurité à la charge du responsable du traitement des données personnelles. Le responsable du traitement est, « sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses

moyens » (Article 3 de la loi relative à l'informatique, aux fichiers et aux libertés) Il s'agit de l'usager ou du fabricant d'objets connectés dans le cadre de l'internet des objets. Cependant, il y a un réel problème dans la législation actuelle quant à la détermination précise, du véritable responsable du traitement. En effet, dans le cas ou le fabricant ne laisse pas le choix à l'utilisateur de protéger ses données correctement. Lorsque le fabricant, collecte des données non consenties par l'utilisateur à l'origine. Il doit être établi sur le territoire français ou recourir à des moyens de traitement situés sur ce territoire. C'est à lui de veiller au respect de la loi Informatique et Libertés en déclarant les traitements sous sa responsabilité au correspondant informatique et libertés (ou à la CNIL si nécessaire) ainsi que leur modification ou suppression. Le droit ordonne à ce dernier de prendre toutes les précautions utiles non seulement quant à la nature des données personnelles mais également quant aux risques liés à leur traitement. Ceci, aussi bien pour préserver la sécurité des données que pour empêcher toute déformation ou endommagement de celles-ci ou bien encore, pour éviter qu'une autre personne puisse y avoir accès sans autorisation préalable. Or, si le responsable du traitement manque à son obligation de sécurité, c'est la vie privée des utilisateurs qui sera mise en danger notamment à travers le profilage intrusif, l'analyse comportementale et encore bien d'autres travers que représentent les objets connectés. Ainsi, relativement à l'application de cet article, le non respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende par l'article 226-17 du code pénal. Lorsque c'est une personne morale qui est en cause, l'amende peut être multipliée par 5 et atteindre jusqu'à 1 500 000 €. Ces obligations vont se développer à travers l'instauration du nouveau projet de règlement Européen.

Cependant, cette obligation de sécurité ne s'avère pas assez stricte. C'est la raison pour laquelle le nouveau projet de loi de règlement Européen va l'améliorer notamment à travers des obligations étendues quant à la notification en cas de failles.

Par ailleurs, une obligation d'information pèse sur le responsable de traitement. En effet d'après l'article 32 de la loi du 6 janvier 1978, toute personne a un droit de regard sur ses données. Ainsi toute personne est en droit de savoir si ses données font l'objet d'un traitement, si elle est fichée et dans quel fichier elle est recensée. En clair, toute personne mettant en œuvre un fichier ou un traitement de données personnelles se doit d'informer les personnes fichées de son identité, de l'objectif et de la collecte d'information. Mais également des destinataires de ces informations. Ce droit est essentiel car il conditionne d'autres droits tels que le droit d'accès ou le droit d'opposition. A ce titre l'affaire récente du téléviseur LG, qui donnait des informations sur ses utilisateurs alors que ceux-ci l'ignoraient illustre une faille dans l'application de cette obligation d'information. En effet, un concepteur de logiciel anglais, avait découvert que le téléviseur espionnait les téléspectateurs. Cela se faisait à travers la publicité qui permettait une collecte de leurs données. Or, en désactivant cette option, il s'est rendu compte que la collecte se faisait toujours mais par une clé USB branchée sur son téléviseur. Cette anecdote ayant fait le tour du monde, ne rassure pas les consommateurs sur la question de l'anonymat appuyée également par les conclusions du G29. Le pouvoir de ces objets sur notre vie quotidienne inquiète car il s'apparente à une forme d'espionnage domestique.

D'autre part, la protection des données personnelles dans le cadre de l'Internet des objets est également assurée à l'échelle transfrontière. En effet, la mondialisation et le développement des nouvelles technologies n'ont fait qu'accroitre le transfert des données à caractères personnels en dehors de France ; ce qui nécessite un encadrement strict en la matière.

C/ Une protection insuffisante des flux transfrontières

Les entreprises d'objets connectés ne cessent de se multiplier face à la révolution du web 3.0. Une étude montre que les français achèteront environ 2 milliards d'objets connectés dans les cinq années à venir[30]. Cependant, au-delà de la France, les entreprises de ces objets dits intelligents sont localisées dans le monde entier. On peut citer Google qui commence à créer des objets intelligents comme les « Google glasses » mais également Amazon qui a créé une télécommande connectée nommée « dash »[31]. La révolution 3.0 ne laisse personne indifférent. C'est la raison pour laquelle la législation en la matière doit être très rigoureuse. La loi relative à l'informatique, aux fichiers et aux libertés assure ainsi une protection des données personnelles des utilisateurs d'objets connectés à l'échelle transfrontière en encadrant strictement le transfert des données hors de l'Union Européenne.

La loi pose le principe à l'article 68, interdisant le transfert des données en dehors des Etats non membres de l'Union Européenne[32].

Cependant, ce principe revêt des exceptions prévues par l'article 69 de la même loi. En effet, on compte trois exceptions dans lesquelles les données personnelles des consommateurs d'objets connectés pourront être transférées hors de l'UE[33].

Tout d'abord légalement, si le pays récepteur présente un niveau de protection suffisant appuyé par une décision de la Commission européenne. C'est le cas notamment de pays tels que la Suisse, le Canada, l'Argentine. De manière contractuelle, par la signature de clauses contractuelles types adoptée par la Commission européenne entre le pays importateur et le pays exportateur de données à caractère personnel ou par l'adoption de règles internes d'entreprise (BCR) qui constitue un code de conduite en ce qui concerne les transferts de données. Enfin, le transfert de données pourra s'effectuer à destination d'une entreprise ayant adhéré au Safe Harbor. Il s'agit d'une convention négociée entre le département du commerce des Etats Unis et la Commission Européenne en 2001. Les entreprises établies aux Etats Unis adhérant à cette convention sont autorisées à recevoir des données en provenance de l'UE. Par exemple la société Apple qui va commercialiser l'Apple Watch en Europe est habilitée à recevoir les données personnelles des utilisateurs de cet objet.

---

[30] CLUNY (D.), « Les français achèteront 2 milliard d'objets connectés dans les 5 ans », *Latribune.fr*, 4 février 2015
[31] FRANK (T.), « Rétrospective 2014 : l'année des objets connectés », *Intelligencentreprises.wordpress.com*, 22 décembre 2014
[32] MATTATIA (F.), *Traitement des données personnelles*, Paris, 2013, Eyrolles, p. 156
[33] CNIL, *Les transferts de données à caractère personnel hors de l'Union européenne*, novembre 2012, p. 5 et 6

Plus précisément cet accord repose sur divers arrangements. Les entreprises adhérant à cet accord doivent tout comme le droit français le permet, garantir certains droits aux individus ayant transmis leurs données personnelles. Concernant la sécurité dont doivent faire preuve les entreprises, celles-ci devront prendre les mesures nécessaires visant la protection des informations qu'elles collectent, contre la suppression, le mauvais usage, la divulgation ou l'altération de ces données. Par ailleurs, les entreprises doivent s'engager à utiliser les données conformément aux finalités pour lesquelles elles ont été collectées. Un contrôle sera mis en place au sein des entreprises, ce qui leur permettra de vérifier que toutes ces règles soient respectées. Il sera également possible, le cas échéant, de faire appel à une entreprise tierce pour effectuer ce contrôle.

Or, ce système de protection a montré ses failles à la suite du scandale des écoutes de l'agence américaine de sécurité nationale NSA. Cette agence ayant demandé à Facebook, Google et à Amazon de lui transmettre des listes de données personnelles, a vu son souhait exhaussé ; ce qui discrédite le Safe Harbor. Suite à cette affaire, le parlement européen a demandé la suspension de cet accord.

Le problème de la protection des données se pose également quant aux mineurs. Or, la législation, dans ce domaine ne présente pas le même niveau de protection en France et aux Etats Unis.

D/ Des carences quant à la protection des données personnelles des mineurs

La protection des données personnelles des mineurs en France est bien moins avancée qu'aux Etats Unis. En effet, les Etats-Unis sont le pays le plus en pointe puisqu'il est à ce jour, l'un des premiers dotés d'une législation concernant Internet et les mineurs.

La loi dite COPPA (Children's Online Privacy Protection Act) a été approuvée le 19 octobre 1999 et, est rentrée en vigueur le 21 avril 2000. Cette loi fédérale sur la protection de la vie privée des enfants de moins de treize ans est contrôlée par le Federal Trade Commission. Cette dernière est très contraignante, interdisant à tout détenteur de site de collecter des données personnelles auprès d'enfants de moins de treize ans sans autorisation parentale préalable. C'est la raison pour laquelle les mineurs ne peuvent pas s'inscrire sur Facebook ou Instagram avant l'âge de 13 ans. En ce qui concerne le traitement et la collecte des données, celles-ci doivent être clairement définis. Les données recueillies auprès des enfants doivent être précisées ainsi que l'usage qui en sera fait ou bien les cessions envisagées. Cette limite de 13 ans ne semble pas pour l'instant avoir son équivalent dans la législation française. En effet, la loi du 6 janvier 1978 ne comporte aucune disposition relatives aux mineurs, ne prévoyant ainsi aucune sanction dans le cas où un les données personnelles d'un mineurs feraient l'objet d'une utilisation frauduleuse. Face à ce manque législatif, la CNIL a fait à ce titre des

propositions dans le cadre du projet de loi numérique[34]. Le but est de modifier la loi actuelle tout en respectant le futur projet de règlement européen, la directive 95/46/CE ainsi que la portée économique de la législation sur les données personnelles entre les pays membres de l'Union Européenne. En effet, à l'heure actuelle, la majorité des mineurs passe un temps considérable sur Internet, notamment sur les réseaux sociaux, étant ainsi concerné tout autant que les adultes par les questions d'e-réputation. De plus, ces derniers utilisent tout autant que les adultes si ce n'est même d'avantage, des objets connectés tels que les tablettes. En effet, d'après les instituts d'études, en 2013 près de 1 million de tablettes pour juniors ont été vendus, représentant 16% du marché. La proportion d'enfants de 7 à 14 ans possédant une tablette est passée de 4 % en 2011 à 33 % en 2013. Ils y jouent au moins une fois par semaine et chaque prise en main dure en moyenne 40 minutes[35]. À ce jour les statistiques ne cessent d'augmenter, c'est la raison pour laquelle une protection à ce niveau est impérative. Ainsi, la CNIL proposerait d'introduire un effacement, notamment en ligne, de données à caractère personnel des mineurs, via l'exercice du droit d'opposition. Cette protection pourrait prendre la forme d'un droit à l'oubli systématique pour toutes les données collectées et traitées ou mise en ligne avant la majorité des mineurs concernés.

Par ailleurs, la protection actuelle octroie une série de droit permettant aux utilisateurs d'avoir un réel droit de regard sur leurs données personnelles, leur permettant de s'informer à ce titre des traitements dont elles font l'objet mais également de leur devenir.

II/ L'encadrement législatif des prétentions des utilisateurs sur leurs données personnelles

Les prétentions des utilisateurs sont encadrées par des droits classiques mis en place par la loi relative à l'informatique, aux fichiers et aux libertés (A). La protection a également fait un pas par la reconnaissance du vol des données personnelles (B) et d'une propriété de ces dernières (C).

A/ Des droits classiques garantis aux individus sur leurs données personnelles

Les utilisateurs d'objets connectés possèdent des droits sur leurs données personnelles définis dans les articles 38 à 40 de la loi de 1978. Cependant, la CNIL souhaite renforcer ces droits qui selon elles sont actuellement trop peu utilisés.

Tout d'abord, chaque utilisateur bénéficie d'un droit d'opposition[36]. Définit à l'article 38, il permet à tout individu de s'opposer, pour des motifs légitimes à ce que ces données soient

[34] CNIL, *Proposition de la CNIL sur les évolutions de la loi informatique et libertés dans le cadre du projet de loi numérique*, 13 janvier 2015, p. 3
[35] BLOCH-SITBON (N.) et DARD (C.), « Le top des tablettes pour enfant : notre sélection », *01net.com*, 18 décembre 2013
[36] MATTATIA (F.), *op.cit*, p. 21

traitées. Ce refus peut s'exprimer de diverses manières. En effet, il peut s'agir d'un refus de répondre lors d'une collecte non obligatoire de données, un refus de donner l'accord écrit obligatoire pour le traitement de données sensibles comme par exemple celles relatives aux convictions religieuses de la personne. C'est également le fait de demander la radiation des données contenues dans des fichiers commerciaux. Et enfin la possibilité de s'opposer à la cession ou la commercialisation d'informations, notamment par le biais d'une case à cocher dans les formulaires de collecte, ceci renvoyant aux systèmes de l'*opt in* et l'*opt out*. Le droit d'opposition s'exerce au moment de la collecte des données ou plus tard en s'adressant au responsable du fichier.

Par ailleurs, tout consommateur justifiant de son identité dispose d'un droit d'accès[37]. L'article 39 de la loi de 2004, permet en effet à tout utilisateur, s'il justifie de son identité d'interroger le responsable d'un traitement de données a caractère personnel afin de savoir ce que ce dernier détient sur lui. Il peut ainsi s'informer des finalités de traitement, du type de données enregistrées, de l'origine et des destinataires et données mais également des éventuels transferts de ces informations vers des pays n'appartenant pas à l'Union Européenne.

Enfin, un droit de contestation est envisagé à l'article 40 de ladite loi[38]. Chaque utilisateur peut s'il justifie de son identité, exiger du responsable de traitement que ses données soient rectifiées, complétées, mises à jour, verrouillées ou effacées du moment que celles-ci sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Cependant, toujours dans le cadre du projet de loi numérique, la CNIL propose de renforcer le droit des personnes[39]. Celle-ci considère que le droit d'accès est trop peu utilisé alors qu'il est le plus important. En effet, il permet à tout individu de savoir ce que le responsable détient sur lui. Ainsi, d'après les volontés de la CNIL, ce droit pourrait être renommé « droit à la connaissance de ses données » ou bien encore « droit à la transparence des données ». Un renforcement de ce droit serait envisagé non seulement dans son contenu mais également dans ses modalités. En effet, dans son contenu, l'article 39 de la loi pourrait être modifié pour donner aux individus un accès relatif aux durées de conservation mais également de manière systématique sur l'origine de leurs données, sur une demande effectuée auprès du responsable de traitement. Concernant les modalités, En ce qui concerne les modalités, il est proposé d'introduire de manière explicite, dans une logique de simplification, la possibilité pour les individus d'exercer les droits prévus des articles 38 à 40 précités aussi par voie électronique. Ceci n'entrainant pas plus de risques de fraudes que de le faire par demande écrite qui pour être recevable doit être accompagné d'un titre identité. La CNIL souhaiterait introduire une obligation à la charge du responsable de traitement de transmettre aux personnes une preuve de l'exercice de leur droit. Par exemple, permettre aux personnes exerçant leur droit

[37] MATTATIA (F.), *op.cit*, p. 45
[38] MATTATIA (F.), *op. cit*, p. 46
[39] CNIL, *op. cit.,* p. 3

d'opposition via un lien de désabonnement de recevoir un email prouvant l'exercice de ce droit constitutif d'une preuve en cas de non-respect de celui-ci.

B/ Une reconnaissance récente du vol de données personnelles

Les objets connectés envahissent notre quotidien en facilitant la vie des consommateurs mais sont cependant vulnérables aux attaques des hackers et cyber pirates.

Le dernier rapport de l'Office Européen de police, en septembre 2014 met en exergue le fait que ces objets fabriqués souvent sans aucune considération de sécurité, fonctionnent avec des logiciels qui peuvent être facilement piratés, ce qui entraine un risque important du vol des données à caractère personnel.

A ce titre, la jurisprudence a eu quelques difficultés à retenir la qualification de vol de données personnelles considérant au départ le fait de voler comme la soustraction d'une chose. Par de nombreux revirements, il s'avère qu'aujourd'hui, la Cour de cassation condamne le vol de données informatiques. En effet, dans une affaire du 22 octobre 2014, la Cour de cassation amorce l'idée selon laquelle les données personnelles sont des biens, ce qui permet plus facilement d'évoquer la notion de vol pour les différents cas relatifs au web 3.0. Mais celle-ci ne précise pas comment l'incrimination de vol doit s'appliquer.

Cependant, d'autres solutions juridiques existent pour déposer plainte dans le cas du vol de données à caractère personnel. Il est possible de recourir à l'article 226-18 du code pénal qui prévoit une peine de cinq ans d'emprisonnement et une amende de 300 000 euros pour celui qui collecte des données par un moyen frauduleux, déloyal ou illicite. Or, l'évolution vers la reconnaissance du « vol » des données vient de faire un nouveau pas par la nouvelle loi antiterroriste du 13 novembre 2014 qui modifie l'article 323-3 du code pénal. Alors que celui-ci réprimait jusqu'ici l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression, il est désormais réprimé « d'extraire, de détenir, de reproduite ou de transmettre » de manière frauduleuse les données. La sanction ici s'élevant à cinq ans de prison et 75 000 euros d'amende et est portée à 7 ans et 100 000 euros s'il s'agit de données personnelles volées dans un système informatique d'état.

Ainsi la nouvelle rédaction de l'article 323-3 permet de réprimer efficacement à l'avenir les vols de données. En ce sens, cette reconnaissance juridique est un premier pas face aux diverses dangers inhérents à l'utilisation des objets connectés.

D'un point de vue juridique, les avancées vont plus loin vers une reconnaissance d'une propriété des données personnelles.

C/ Vers la reconnaissance d'une propriété des données personnelles

À l'heure actuelle, en droit Français, les données personnelles des individus ne sont pas considérées comme des propriétés, mais comme un droit attaché à la personne humaine et au respect qui lui est dû. Les données personnelles relèvent des droits de la personnalité. Ces droits de la personnalité sont extrapatrimoniaux, à ce titre ils ne sont pas évaluables en argent. Il convient de dire que ces droits sont inaliénables, incessibles et imprescriptibles. Mais, en dépit de leur caractère ces données personnelles constituent une importante manne financière et participent à l'enrichissement de ceux qui participent à leur traitement.

En effet, dans le cadre de l'internet des objets, les données collectées par les différents périphériques peuvent établir le profil précis d'un utilisateur, une vision très détaillée de ses centres d'intérêts, de ses besoins… Ces données sont très précieuses afin de proposer aux utilisateurs des produits et services correspondants à leurs exigences. De plus, toutes ces données constituent une base que l'industriel peut également revendre à des annonceurs. Ces derniers pourront alors utiliser ces différentes données afin d'affiner leurs campagnes de publicités en ciblant plus précisément leurs consommateurs potentiels. C'est pourquoi il est courant de désigner les données personnelles comme étant le nouveau « pétrole numérique », du fait de leur importante valeur économique.

Cependant, l'utilisateur partage gratuitement ses données personnelles à un industriel qui les revend par la suite. Face à un tel constat, ces dernières années plusieurs voix se sont élevées afin de réclamer une patrimonialisation des données personnelles afin de retrouver plus d'équilibre dans les échanges et d'écarter l'image d'une exploitation abusive et unilatérale des données personnelles.

Lorsqu'on parle de patrimonialisation comme le souligne Thomas St-Aubin, on parle plutôt d'un droit à la réutilisation[40]. Un droit de mobiliser, d'enrichir et de distribuer ses données personnelles. Cela nous conduit à une forme de monétisation, de commercialisation des données personnelles. A ce titre un sondage Havas[41] de septembre 2014 tend à confirmer cette tendance. En effet, 45% des internautes selon ce sondage sont prêts à partager leurs données moyennant des contreparties financières et 30% estiment que 500 euros seraient suffisant pour un partage intégral pendant un an. Cette volonté de monétiser ses données personnelles, certains l'ont déjà compris, c'est le cas notamment d'une start-up, « Publi-addict » qui propose en échange de nos données personnelles une rémunération pouvant aller jusqu'à 300 euros par mois. Le principe est le même que sur n'importe quel réseau social excepté qu'ici il y a une contrepartie financière au fait de consulter la publicité ciblée. En d'autres termes, ce n'est pas directement la vente de données personnelles qui est rémunéré, mais le fait de consulter de la publicité en conformité avec les données personnelles que l'on a partagé.

---

[40] SAINT-AUBIN (T.), « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) - Les droits de l'opérateur de données sur son patrimoine numérique informationnel », RLDI, mars 2014, numéro 102, p.3

[41] HAVAS MEDIA, *op. cit.,* p. 35 et 38

Dans le cadre de l'internet des objets il suffira de partager les informations collectées par les différents périphériques avec ce genre de plateformes appelées à se multiplier afin de monétiser nos données personnelles. À ce titre, le droit à la portabilité des données est un volet important du projet de règlement européen sur les données personnelles[42]. L'article 18 de ce projet de règlement confère à l'utilisateur le droit à la portabilité de ses données, c'est-à-dire le droit de transmettre des données d'un système de traitement à un autre, sans que le responsable du traitement ne puisse y faire obstacle.

Ainsi, sans être un droit patrimonial sur les données personnelles, il permet à un individu de reprendre le contrôle sur ses données. C'est la reconnaissance d'un droit d'appropriation de l'individu sur ses données personnelles. Le traitement des données personnelles sera moins unilatéral, l'utilisateur aura le droit de récupérer ses informations pour les utiliser sur une autre plateforme. Mais, un effet pervers semble se profiler, car l'industriel qui aura investi dans un périphérique captant des données personnelles bien spécifiques pourra voir le bénéfice de son investissement être transféré vers une autre plateforme. L'industriel n'aura alors plus l'assurance de l'exclusivité des données qu'il collecte. Cependant pour les utilisateurs ce droit de portabilité est un bon compromis à la reconnaissance d'un droit patrimonial sur les données personnelles. D'autant plus que le Conseil National du Numérique a dans son dernier rapport sur la neutralité des plateformes[43], déconseillé la reconnaissance d'un tel droit préférant la reconnaissance d'une portabilité des données. Le conseil a justifié sa position en trois points :

- Car elle renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises.

- Parce qu'elle ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques.

- Parce qu'elle déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et les autres.

Qui plus est, comme le souligne Thomas Saint-Aubin, *« Un droit de propriété implique un droit d'être dépossédé, alors qu'un droit de la personnalité est inaliénable ».* Ainsi, la patrimonialisation des données serait une régression pour les individus. Le fait que les données personnelles soient aujourd'hui attachées à la personne reste la garantie d'une protection efficace. Il serait dommage de troquer la protection des individus dans la perspective d'intérêts mercantiles. Cependant, si les individus se sentent aujourd'hui déposséder de leurs données personnelles, la reconnaissance prochaine d'un droit de portabilité des données personnelles viendra

[42] COMMISSION EUROPÉENNE*, La protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* proposition de règlement de la Commission Européenne, n° 2012/0011, 25 janvier 2012, p.59

[43] CONSEIL NATIONAL DU NUMÉRIQUE, *Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014, p.36-37

renforcer leur sentiment d'appropriation sur ces données dont ils pourront désormais disposer avec une plus grande liberté.

Face à l'essor de la révolution du web 3.0 et de la multiplication d'objets connectés à venir, il s'avère que la loi relative à l'informatique, aux fichiers et aux libertés présente des limites dans les domaines évoqués précédemment. Ainsi, au-delà des propositions de la CNIL en vue d'une modification de la législation actuelle, un projet de règlement européen est à l'étude afin de pallier aux manquements de la législation actuelle.

SECTION III/ UN ENCADREMENT DE l'INTERNET DES OBJETS RENFORCÉ PAR L'INSTAURATION D'UN REGLEMENT EUROPÉEN RELATIF AUX DONNÉES PERSONNELLES

Comme nous l'avons vu précédemment les objets connectés auront un impact sans précédent sur le traitement de nos données personnelles. Si le droit apporte aujourd'hui des solutions à certaines problématiques relatives aux données personnelles, des évolutions sont nécessaires afin d'appréhender au mieux ce web 3.0. Pour ce faire, un projet de u relatif à la protection des données personnelles est à l'étude. Ce projet vise à harmoniser et moderniser le cadre législatif relatif aux données personnelles devenu en partie obsolète depuis la directive de 1995. Ce projet comporte notamment plusieurs mesures qui devront s'appliquer aux responsables du traitement allant ainsi vers un encadrement total du processus de traitement des données personnelles (I). Mais, ce projet de par l'importance des sanctions qu'il préconise et des conséquences qu'elles peuvent engendrer préfigure d'un respect impératif et ceux notamment pour les entreprises de l'internet des objets. (II)

I/ Vers un encadrement total du processus de traitement des données personnelles

Ce projet de règlement préconise une protection étendue des données personnelle. En effet, avec l'instauration des concepts d'Accountability (A) et de Privacy by Design/ by Default (B) c'est un véritable quadrillage en amont et en aval du traitement des données personnelles que tente de mettre en œuvre ce projet de règlement.

A/ L'instauration du concept d'Accountability pour un contrôle en aval du traitement des données personnelles

L'Accountability est un concept présent à l'article 22 de ce projet de règlement sans pour autant être nommé explicitement[44]. En français on peut traduire ce concept par responsabilité. L'Accountability s'inscrit dans une démarche de transparence, c'est une situation dans laquelle le responsable du traitement doit rendre des comptes et répondre de sa conduite[45]. Il s'agit de retirer toute opacité dans le traitement des données personnelles. La mise en pratique de ce concept est également la contrepartie de la disparition d'un régime préventif basé sur l'obligation de déclaration préalable pour basculer vers un régime répressif basé sur plus de responsabilité. En effet, encore aujourd'hui, une entreprise qui désire traiter des données doit se déclarer auprès de la CNIL, face à une explosion des données

[44] *La protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, proposition de règlement de la Commission Européenne, n° 2012/0011, 25 janvier 2012, p.61

[45] BENSOUSSAN (A.), « Accountability et réformes des données personnelles », *alain-bensoussan.com*, le 15 janvier 2014

personnelles, ce régime de déclaration n'est plus souhaitable. Désormais, en contrepartie, le responsable du traitement devra adopter des règles internes et mettre en œuvre des mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement. On tente de responsabiliser le responsable du traitement.

Afin de respecter ce principe, l'article 22 du projet de règlement préconise le respect de plusieurs mesures telles que :

- La tenue d'une documentation/d'un registre retraçant tous les traitements de données à caractère personnelles (Art 28). C'est une exigence qui facilitera les contrôles a posteriori et qui témoigne d'une véritable politique de transparence. Cependant pour les entreprises cette obligation se traduit comme une contrepartie très lourde à l'absence de déclaration.

- La nécessité d'assurer un niveau de sécurité adapté aux risques présentés par le traitement et à la nature des données à caractère personnel à protéger (Art 30). Il est devenu commun de désigner les données personnelles comme le nouveau « pétrole numérique », ces données ont une réelle valeur marchande. Ainsi il est dans l'intérêt de l'entreprise de sécuriser les données qu'elle a recueilli et de ne pas les divulguer facilement. Pour faire le parallèle avec une banque, le client confie à une société ses données personnelles à charge pour elle de les protéger, ces données ne doivent pas être éparpillées dans la nature. Par ailleurs, la garantie de la protection des données personnelles est aussi un argument commercial important pour influer sur le choix d'un consommateur sur tel ou tel produit.

- La désignation d'un délégué à la protection des données pour toutes entreprises de plus de 250 employés. (Art 35) En France il existe déjà des correspondants informatique et liberté mais jusqu'à maintenant leur présence n'est pas obligatoire. Il y aura donc dans ces entreprises un relais compétant pour comprendre toutes les problématiques relatives aux données personnelles et ainsi éviter toutes dérives dans le traitement de ces données.

Cependant, le concept d'Accountability n'est pas la seule évolution amenant à une meilleure protection des données personnelles.

B/ L'instauration des concepts de Privacy pour un contrôle en amont du traitement des données personnelles

Ces deux concepts souvent synonymes s'inscrivent également dans une politique de renforcement de la protection des données personnelles. Ces deux concepts que l'on peut traduire par protection des données dès la conception et protection des données par défaut, se trouvent à l'article 23 du projet de règlement sur les données personnelles. Ce sont des

concepts complémentaires avec celui d'Accountability que le projet de règlement entend établir. Il s'agit de quadriller le traitement des données personnelles pour plus de protection. En effet, si l'Accountability est un concept qui prend en compte la protection des données personnelles en aval, à l'inverse les concepts de Privacy by design et by default prennent en compte la protection des données personnelles en amont du traitement.

Cependant s'ils participent de la même logique le Privacy by design et by default sont différents. Le Privacy by default a été défini par la commissaire européenne Viviane Reding[46]. Selon sa définition, ce concept vise à éviter une exploitation détournée des données à des fins autres que celles pour lesquelles une personne avait initialement donné son consentement. C'est l'idée d'offrir à l'utilisateur le plus haut niveau de protection en matière de données personnelles[47]. L'article 23 du projet de règlement associe au concept de Privacy by default les principes de finalité et de péremption des données traitées pour illustrer cette nécessité d'offrir à défaut le plus haut niveau de protection. En effet, selon l'article 23, « *par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités* ». On est dans une logique de opt-in, c'est-à-dire que le consentement explicite de l'utilisateur doit être demandé pour chaque utilisation autre que pour celle consenti à l'origine.

Quant à la notion de Privacy by design ou de protection des données dès la conception, c'est une notion à la base Canadienne[48], elle consiste à prendre en compte des exigences en termes de protection des données personnelles dès la conception du produit. C'est l'articulation entre des standards juridiques et techniques. La protection des données personnelles doit être intégrée à la technologique. Cette notion a été reprise par le comité du G29[49] ainsi que lors de la dernière conférence annuelle des commissaires à la vie privée et à la protection des données[50].

Dans le projet de règlement européen, l'article 23 mentionne des mécanismes qui permettent de ne pas rendre accessible à n'importe qui les données personnelles que l'entreprise est susceptible de traiter. Pour le moment cette notion reste très vague mais on semble entrevoir des applications futures de ce concept tel que celui du « silence des puces ».

Comme nous l'avons vu précédemment, l'internet des objets va conduire les individus à être connecté en permanence. Les individus seront en interaction permanente avec ces objets qui collecteront sans cesses leurs données personnelles. Mais, les objets seront eux-mêmes interconnectés entre eux notamment grâce à la technologie de radio-identification ou RFID.

---

[46] REDING (V.), *Your data, your rights: Safeguarding your privacy in a connected world*, discours prononcé à Bruxelles le 16 mars 2011.
[47] SCHWAAD (J-C.), « Savoir ce qu'est le Privacy by design et le Privacy by default », *www.cil.cnrs.fr*, mise en ligne le 24 novembre 2014.
[48] CAVOUKIAN (A.), *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, www.privacybydesign.ca, décembre 2012, p72.
[49] G29, *op. cit.*, p.3
[50] KOHNSTAMM (J.) et MADHUB (D.), *Mauritius Declaration on the Internet of Things*, 14 octobre 2014, p.2.

La technologie RFID pour *Radio Frequency Identification* permet de récupérer des données à distance grâce à une puce implantée sur un objet. Pour prendre un exemple concret, il suffit qu'un smartphone équipé d'un lecteur de puces RFID passe à côté d'un objet connecté pour récupérer les données personnelles qu'il est susceptible d'avoir recueillies. Ce « scan furtif » a aussi fait la une de l'actualité à propos de la mise en place future de panneaux publicitaires connectés. Ainsi, lorsqu'on passera à proximité d'un panneau publicitaire, ce dernier pourra récolter les données recueillis par nos différents objets connectés (smartphone, montre, voiture…) et proposer une publicité ciblée instantanément.

Ainsi, sans rentrer dans une psychose mal venue, la meilleure protection pour l'individu ne serait-ce pas une meilleure maitrise de ces interactions ? C'est pour cette raison, qu'il est de plus en plus mis en avant un droit à la déconnexion ou bien encore un droit au « silence de la puce ». Des prémisses de ce droit étaient présentes en 2009 dans une recommandation sur l'utilisation de ces RFID délivré par commission européenne[51]. Cette recommandation préconisait notamment la désactivation des étiquettes RFID que l'on peut trouver dans le commerce sur certains produits dès l'achat.

Appliqué aux objets connectés, ce droit reviendrait pour un individu à avoir la certitude que les objets connectés autour de lui ne divulguent aucune information le concernant sans son consentement. Cela reviendrait à revenir à une utilisation « normale » d'un objet[52]. Concrètement, l'intégration par exemple d'un bouton ON/OFF permettant la déconnexion de l'utilisateur serait une mesure techniques qui serait en accord avec le principe de Privacy by design. En effet, si un industriel offre dès la conception du produit la possibilité pour l'utilisateur de l'utiliser hors-ligne en dehors de toutes interactions cela reviendrait à respecter ce droit au « silence de la puce » et constituerait le parfait exemple concret d'une mise en pratique du Privacy by design. D'ailleurs en 2009 la recommandation de la commission européenne faisait déjà le parallèle entre les deux notions en préconisant, d'intégrer des fonctions de sécurité de l'information et de respect de la vie privée dans les applications RFID avant leur diffusion généralisée en conformité avec le principe de «sécurité et respect de la vie privée assurés dès la conception».

Pour autant on peut déjà deviner la valeur ajoutée que peut apporter la mise en pratique d'un tel concept. En effet, si un industriel met en avant le fait que le produit connecté qu'il vend respecte la protection des données personnelles cela va inciter les clients à l'achat. L'industriel aura alors une image de marque associée à une certaine fiabilité. Des éléments, qui incitent à l'achat mais qui peuvent également inciter à un partage accru de données. En effet, l'intérêt pour un industriel au-delà de la simple vente de son périphérique est que les clients qui ont fait l'acquisition de l'objet connecté l'utilisent afin de partager leurs données personnelles. En

[51] REDING (V.), La mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, recommandation de la Commission Européenne, n°2009/387/CE, 12 mai 2009,
[52] DE SILGUY (S.), *op. cit.,* p.66

effet, plus il y aura d'utilisateurs actifs plus les données partagées seront fiables et pertinentes. Une base d'utilisateurs actifs forment une communauté ce qui est un véritable avantage concurrentiel face aux autres acteurs du marché qui peuvent alors souffrir de la comparaison. En définitive le Privacy by design qui est à l'origine une contrainte peut se transformer en réel atout et former un cercle vertueux pour l'industriel.

II/ Vers un respect impératif du règlement pour les acteurs de l'internet des objets

À la lecture de ce projet de règlement il en va de l'intérêt des fabricants d'objets connectés de respecter cette réglementation. En effet, les sanctions préconisées en cas de manquements peuvent porter un préjudice financier très important aux entreprises (A) ainsi qu'une atteinte irrémédiable à l'image de marque de la société (B).

A/ Des sanctions financières portant préjudice à l'économie de l'entreprise

En cas de non-respect des mesures préconisées par le projet de règlement, il faut se rapporter à l'article 79§6 qui énonce de lourdes sanctions pouvant aller jusqu'à 2% du chiffre d'affaire pour une société ou 1 million d'euros. Ce seuil a d'ailleurs été considérablement relevé depuis pour passer de 5% du chiffre d'affaire d'un groupe ou 100 millions d'euros. En cas de sanction, le juge privilégiera la somme la plus élevée entre les deux. Ces sommes sont bien éloignées du montant des sanctions actuelles qui plafonnement à 300 000 euros pour une personne physique ou 1,5 million si c'est une personne morale. (article 226-16 du code pénal)

Une telle inflation dans le montant des amendes allouées sont la contrepartie au fait d'offrir plus de libertés aux responsables du traitement et à leurs sous-traitants. En l'absence d'un régime de déclaration préalable et avec l'instauration d'un régime de répressif, les responsables et leurs sous-traitants doivent faire face à leurs responsabilités.

De plus, le montant de ces sanctions prend également compte les revenus pharamineux qui peuvent découler de l'activité de traitement des données personnelles. En effet, la sanction d'1 million d'euros prévue initialement pouvait sembler trop peu dissuasive pour les entreprises des GAFA dont le chiffre d'affaire se calcule en milliards d'euros.

Le montant de ces sanctions peut également se justifier du fait des nouveaux dangers qui gravitent autour des données personnelles et qui nécessite une plus grande vigilance. Pour cette raison, les négligences et les manquements des entreprises sont sanctionnées avec une plus grande fermeté afin d'encourager à garantir au mieux la protection des données

personnelles. Ainsi au-delà du « portefeuille » des sociétés c'est à leur image de marque et à leur réputation que le projet de règlement désir s'attaquer en cas de manquement.

B/ Des obligations de notification portant préjudice à la réputation de l'entreprise

Le projet de réglementation prévoit également un élargissement de l'obligation de notification en cas de violation de données à caractère personnelles à tous les responsables de traitements de données personnelles. Jusqu'ici, en vertu de l'article 34 de la loi de janvier 1978, l'obligation de notification à la CNIL en cas de violation de données à caractères personnelles ne concernait que les fournisseurs de services de communications électroniques au public (article 34-bis de la loi du 6 janvier 1978). Dans ce projet de règlement, l'article 31 relatif à l'obligation de notification ne semble pas faire de distinctions, il y a une volonté d'imposer la notification à chaque « responsable du traitement ». Ainsi, les sociétés développant des objets connectés qui échappaient jusqu'ici à cette obligation de notification devront la respecter si le règlement est adopté en l'état.

De plus comme l'indique l'article 32, il doit également y avoir une communication à la personne concernée d'une violation de données à caractère personnelle. Cette exigence s'inscrit au même titre que le concept d'Accountability dans une politique de transparence. Les individus qui confient leurs données personnelles doivent être au courant de toute utilisation et de tout défaut dans leur traitement.

Ainsi, l'élargissement de l'obligation de notification au « responsable du traitement » ainsi que l'obligation de communication aux personnes, participent indirectement au renforcement de la protection des données personnelles. En effet, les conséquences peuvent être catastrophiques pour une entreprise si elle est contrainte de notifier à l'autorité compétente ainsi qu'à ses clients une violation des données personnelles qu'elle est censée devoir protéger. Une telle situation égratignera irrémédiablement son image de marque. On est encore une fois dans cette logique de cercle vertueux, un industriel a donc tout intérêt à éviter cette situation en renforçant son dispositif de sécurité. A ce titre, la présidente de la CNIL Isabelle Falque-Pierrotin a souligné très justement que le respect du droit des données personnelles ne doit pas être vu comme une contrainte au contraire, car « *La fiabilité dans la protection des données personnelles est une exigence commerciale et économique déterminante et un avantage concurrentiel* »[53]

[53] FALQUE-PIERROTIN (I.), *Quelle protection européenne pour les données personnelles ?,* Question d'Europe n°250*, Fondation Robert Schuman*, 3 septembre 2012, p.3

BIBLIOGRAPHIE

OUVRAGES GÉNÉRAUX

- LE PETIT ROBERT, *Le Robert*, Paris, 2013

OUVRAGES SPÉCIALISÉS

- GENTOT (M.), « la protection des données personnelles à la croisée des chemins », sous la direction de TABATONI P., *La protection de la vie privée dans la société d'information*, Tome 3, coll. Cahiers des sciences morales et politiques, PUF, Paris, 2002, 359 p.

- HAAS (G.), et COHEN-HADRIA (Y.), *Guide juridique informatique et libertés – Collecte, traitement et sécurité des données dans l'univers numérique : ce que vous devez savoir*, ENI, Saint-Herblain, 2012, 230 p.

- LEROY (F.), *Réseaux sociaux & Cie – Le commerce des données personnelles*, Actes sud, Arles, 2013, 263 p.

- MATTATIA (F.), *Traitement des données personnelles*, Paris, 2013, Eyrolles, 187 p.

- REY (B.), *La vie privée à l'ère du numérique*, Lavoisier, Cachan, 2012, 297 p.

RAPPORTS & AVIS

- CAVOUKIAN (A.), *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, www.privacybydesign.ca, décembre 2012, 72 p.

- CNIL, *Les transferts de données à caractère personnel hors de l'Union européenne*, novembre 2012, 38 p.

- CNIL, *Proposition de la CNIL sur les évolutions de la loi informatique et libertés dans le cadre du projet de loi numérique*, 13 janvier 2015, 8 p.

- CNIL, *Vie privée à l'horizon 2020*, Cahier IP n°1, 58 p.

- Commission Européenne, *L'internet des objets : un plan d'action pour l'Europe* COM/2009/0278, 18 juin 2009, 12 p.
-
- Commission Européenne, *La protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, n° 2012/0011, 25 janvier 2012, 134 p.

- Conseil National du Numérique, *Neutralité des plateformes : réunir les conditions d'un environnement numérique ouvert et soutenable*, mai 2014, 120 p.

- G29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, avis du 16 septembre 2014, 24 p.

- REDING (V.), *La mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence,* recommandation de la Commission Européenne, n°2009/387/CE, 12 mai 2009, 5 p.

CHARTE

- KOHNSTAMM (J.) et MADHUB (D.), *Mauritius Declaration on the Internet of Things*, 14 octobre 2014, 2 p.

ARTICLES

- DE SILGUY (S.), *Les objets connectés, un risque pour la protection de nos données personnelles*, RDLC, octobre 2014, numéro 119, p. 66-69
-
- FALQUE-PIERROTIN (I.), *Quelle protection européenne pour les données personnelles ?,* Question d'Europe n°250*, Fondation Robert Schuman*, 3 septembre 2012, 9 p.

- FTC., *Internet of things - Privacy & security in a connected world,* FTC staff report, january 2015, 55 p.

- HAVAS MEDIA, *Les français et leurs données personnelles, quelle place pour les marques ?*, septembre 2014, 68 p.

- HP. FORTIFY SECURITY RESEARCH, *Internet of Things Research Study*, HP report, september 2014, 6 p.

- SAINT-AUBIN (T.), *Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel*, RLDI, mars 2014, numéro 102, 12 p.

DOCUMENTS INTERNET

- ANONYME, « INTRUSION 2.0 - Avec Shodan, contrôlez des webcams et imprimez chez les autres », *lemonde.fr*, 10 juin 2014

- BENSOUSSAN (A.), « Accountability et réformes des données personnelles », *alain-bensoussan.com*, le 15 janvier 2014

- BLOCH-SITBON (N.) et DARD (C.), « Le top des tablettes pour enfant : notre sélection », *01net.com*, 18 décembre 2013

- BRETON (J.), « Mots de passe les plus utilisés : le top 25 demeure dominé par le 123456 », *lesnumeriques.com*, 21 janvier 2015

- CHAMPEAU (G.), « Michael Hastings a-t-il été tué par le piratage de sa voiture ? », *numerama.com*, 26 juin 2013

- CLUNY (D.), « Les français achèteront 2 milliard d'objets connectés dans les 5 ans », *Latribune.fr*, 4 février 2015

- DESSIBOURG (O.), « Pirater une voiture ? C'est possible … », *Lemonde.fr*, 4 mars 2014

- FRANK (T.), « Rétrospective 2014 : l'année des objets connectés », *Intelligencentreprises.wordpress.com*, 22 décembre 2014

- FREDOUELLE (A.), « Le marché français des objets connectés pèsera 500 millions en 2016 », *journaldunet.com, 2 mai 2014*.

- JUNG (M.), « Apprenez à mieux gérer vos mots de passe », *bfmtv.com*, 27 janvier 2015

- KRISTANADJAJA (G.), « J'ai pris le contrôle de votre caméra et je vous ai retrouvés », *rue89.nouvelobs.com*, 09 juin 2014

- PINTE (J-P.), « Le vol d'identité, la plus grande menace criminelle des années à venir », *atlantico.fr*, 30 décembre 2013

- PIROTTE (J.), « Shodan : un moteur de recherche pour l'internet des objets », *objetconnecte.net*, 30 mai 2014

- SCHWAAD (J-C.), « Savoir ce qu'est le Privacy by design et le Privacy by default », *www.cil.cnrs.fr*, mise en ligne le 24 novembre 2014.

DISCOURS

- REDING (V.), *Your data, your rights: Safeguarding your privacy in a connected world*, discours prononcé à Bruxelles, 16 mars 2011

SITES INTERNET

- CNRS, www.cil.cnrs.fr

TABLE DES MATIÈRES